Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019110

International filing date: 21 December 2004 (21.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-433904
Filing date: 26 December 2003 (26.12.2003)

Date of receipt at the International Bureau: 17 February 2005 (17.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/JP2004/019110

24.12.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

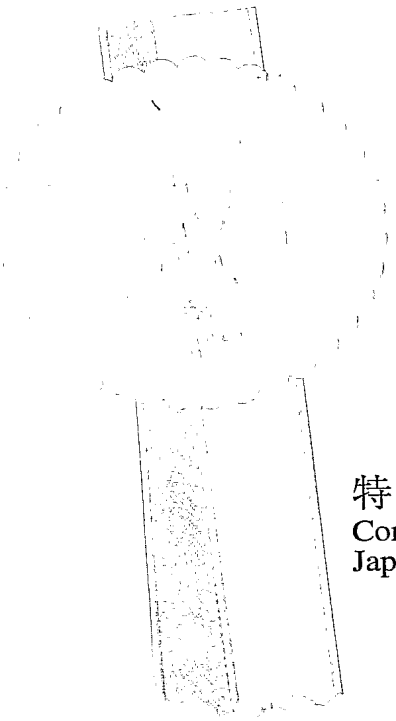
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１２月２６日

出願番号
Application Number: 特願２００３－４３３９０４

[ST. 10/C]: [ＪＰ２００３－４３３９０４]

出願人
Applicant(s): 松下電器産業株式会社



２００５年　２月　４日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３００６７８５

【書類名】　特許願
【整理番号】　2048150095
【提出日】　平成15年12月26日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　5/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　布田　裕一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742

【書類名】特許請求の範囲
【請求項１】
鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムであって、
前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、
前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備えること
を特徴とする鍵発行システム。
【請求項２】
鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムであって、
前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、
前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、
前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備えること
を特徴とする鍵発行システム。
【請求項３】
前記証明書発行サーバは、さらに、前記公開鍵が前記発行識別子に基づいた前記素数を用いて生成されているかを判定する鍵判定部を備えること
を特徴とする請求項２記載の鍵発行システム。
【請求項４】
前記素数生成部は、前記発行識別子情報に基づいて２つの素数を生成すること
を特徴とする請求項１から請求項３のいずれか１項に記載の鍵発行システム。
【請求項５】
前記素数生成部は、前記発行識別子情報ＩＤＩ及び０≦ｃ１，ｃ２＜ＩＤＩを満たす予め与えられた整数ｃ１，ｃ２に対して、Ｎ１＝ｃ１　ｍｏｄ　ＩＤＩ及びＮ２＝ｃ２　ｍｏｄ　ＩＤＩを満たす素数Ｎ１及びＮ２を生成すること
を特徴とする請求項１から請求項３のいずれか１項に記載の鍵発行システム。
【請求項６】
前記鍵判定部は、前記素数Ｎ１及びＮ２の積である前記公開鍵ｎ（＝Ｎ１×Ｎ２）と前記整数ｃ１，ｃ２に対して、ｎ－ｃ１×ｃ２が発行識別子情報ＩＤＩで割り切れることを判定すること
を特徴とする請求項５記載の鍵発行システム。
【請求項７】
前記素数生成部は、第１素数ｑ、乱数Ｒ及び前記発行識別子情報ＩＤＩを用いてＮ＝２×Ｒ×ＩＤＩ×ｑ＋１で表される素数Ｎを生成すること
を特徴とする請求項１から請求項６のいずれか１項に記載の鍵発行システム。
【請求項８】
前記素数生成部は、ｌｅｎビットの素数を生成し、
ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、
乱数Ｒを生成する乱数生成手段と、

前記発行識別子情報ＩＤＩ、前記第１の素数ｑ及び前記乱数Ｒを用いて、Ｎ＝２×Ｒ×ＩＤＩ×ｑ＋１なる素数候補Ｎを生成する素数候補生成部と、
前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、
前記素数候補Ｎ及び前記乱数Ｒに対し、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する第２の素数判定部と、を備えること
を特徴とする請求項１から請求項７のいずれか１項に記載の鍵発行システム（ここで、ａ＾ｘはａのｘ乗を示す）。

【請求項９】
前記素数生成部は、ｌｅｎビットの素数を生成し、
ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、
乱数Ｒを生成する乱数生成手段と、
前記発行識別子情報ＩＤＩ、前記第１の素数ｑ及び前記乱数Ｒを用いて、Ｎ＝２×Ｒ×ＩＤＩ×ｑ＋１なる素数候補Ｎを生成する素数候補生成部と、
前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、
前記素数候補Ｎ及び前記乱数Ｒに対し、ＧＣＤ（２＾（２Ｒ）－１，Ｎ）＝１を満たすか否かを判定する第２の素数判定部と、を備えること
を特徴とする請求項１から請求項７のいずれか１項に記載の鍵発行システム（ここで、ＧＣＤ（Ｘ，Ｙ）はＸとＹの最大公約数を示す）。

【請求項１０】
前記鍵判定部は、前記公開鍵ｎに対して、ｎ－１が前記発行識別子情報ＩＤＩで割り切れることを判定すること
を特徴とする請求項１から請求項９のいずれか１項に記載の鍵発行システム。

【請求項１１】
前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むこと
を特徴とする請求項１から請求項１０のいずれか１項に記載の鍵発行システム。

【請求項１２】
鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置であって、
前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、
前記秘密鍵は発行識別子情報に基づいて生成された複数の素数を含むこと
を特徴とする端末装置。

【請求項１３】
鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置であって、
前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、
前記秘密鍵は発行識別子情報に基づいて生成された複数の素数を含むこと
を特徴とする端末装置。

【請求項１４】
前記秘密鍵は前記発行識別子情報に基づいて生成された２つの素数を含むこと
を特徴とする請求項１２または請求項１３記載の端末装置。

【請求項１５】
前記２つの素数は、前記発行識別子情報ＩＤＩ及び０≦ｃ１，ｃ２＜ＩＤＩを満たす予

め与えられた整数ｃ１，ｃ２に対して、Ｎ１＝ｃ１　ｍｏｄ　ＩＤＩ及びＮ２＝ｃ２　ｍｏｄ　ＩＤＩを満たす素数Ｎ１及びＮ２であること
を特徴とする請求項１２から請求項１４のいずれか１項に記載の端末装置。

【請求項１６】
前記複数の素数は、第１素数ｑ、乱数Ｒ及び前記発行識別子情報ＩＤＩを用いてＮ＝２×Ｒ×ＩＤＩ×ｑ＋１で表されること
を特徴とする請求項１２から請求項１４のいずれか１項に記載の端末装置。

【請求項１７】
鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバであって、
前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備えること
を特徴とする鍵発行サーバ。

【請求項１８】
前記素数生成部は、前記発行識別子情報に基づいて２つの素数を生成すること
を特徴とする請求項１７記載の鍵発行サーバ。

【請求項１９】
前記素数生成部は、前記発行識別子情報ＩＤＩ及び０≦ｃ１，ｃ２＜ＩＤＩを満たす予め与えられた整数ｃ１，ｃ２に対して、Ｎ１＝ｃ１　ｍｏｄ　ＩＤＩ及びＮ２＝ｃ２　ｍｏｄ　ＩＤＩを満たす素数Ｎ１及びＮ２を生成すること
を特徴とする請求項１７または請求項１８記載の鍵発行システム。

【請求項２０】
前記素数生成部は、第１素数ｑ、乱数Ｒ及び前記発行識別子情報ＩＤＩを用いてＮ＝２×Ｒ×ＩＤＩ×ｑ＋１で表される素数Ｎを生成すること
を特徴とする請求項１７から請求項１９のいずれか１項に記載の鍵発行サーバ。

【請求項２１】
前記素数生成部は、ｌｅｎビットの素数を生成し、
ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、
乱数Ｒを生成する乱数生成手段と、
前記発行識別子情報ＩＤＩ、前記第１の素数ｑ及び前記乱数Ｒを用いて、Ｎ＝２×Ｒ×ＩＤＩ×ｑ＋１なる素数候補Ｎを生成する素数候補生成部と、
前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、
前記素数候補Ｎ及び前記乱数Ｒに対し、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する第２の素数判定部と、を備えること
を特徴とする請求項１７から請求項２０のいずれか１項に記載の鍵発行サーバ。

【請求項２２】
前記素数生成部は、ｌｅｎビットの素数を生成し、
ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、
乱数Ｒを生成する乱数生成手段と、
前記発行識別子情報ＩＤＩ、前記第１の素数ｑ及び前記乱数Ｒを用いて、Ｎ＝２×Ｒ×ＩＤＩ×ｑ＋１なる素数候補Ｎを生成する素数候補生成部と、
前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、
前記素数候補Ｎ及び前記乱数Ｒに対し、ＧＣＤ（２＾（２Ｒ）－１，Ｎ）＝１を満たすか否かを判定する第２の素数判定部と、を備えること

を特徴とする請求項１７から請求項２０のいずれか１項に記載の鍵発行サーバ。
【請求項２３】
前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むこと
を特徴とする請求項１７から請求項２２のいずれか１項に記載の鍵発行サーバ。
【請求項２４】
素数を生成する素数生成装置であって、
前記素数生成装置は、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、を備えること
を特徴とする素数生成装置。
【請求項２５】
前記素数生成部は、前記発行識別子情報ＩＤＩ及び０≦ｃ＜ＩＤＩを満たす予め与えられた整数ｃに対して、Ｎ＝ｃ　ｍｏｄ　ＩＤＩを満たす素数Ｎを生成すること
を特徴とする請求項２４記載の素数生成装置。
【請求項２６】
前記素数生成部は、第１素数ｑ、乱数Ｒ及び前記発行識別子情報ＩＤＩを用いてＮ＝２×Ｒ×ＩＤＩ×ｑ＋１で表される素数Ｎを生成すること
を特徴とする請求項２４または請求項２５記載の素数生成装置。
【請求項２７】
前記素数生成部は、ｌｅｎビットの素数を生成し、
ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、
乱数Ｒを生成する乱数生成手段と、
前記発行識別子情報ＩＤＩ、前記第１の素数ｑ及び前記乱数Ｒを用いて、Ｎ＝２×Ｒ×ＩＤＩ×ｑ＋１なる素数候補Ｎを生成する素数候補生成部と、
前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、
前記素数候補Ｎ及び前記乱数Ｒに対し、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する第２の素数判定部と、を備えること
を特徴とする請求項２４から請求項２６のいずれか１項に記載の素数生成装置。
【請求項２８】
前記素数生成部は、ｌｅｎビットの素数を生成し、
ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、
乱数Ｒを生成する乱数生成手段と、
前記発行識別子情報ＩＤＩ、前記第１の素数ｑ及び前記乱数Ｒを用いて、Ｎ＝２×Ｒ×ＩＤＩ×ｑ＋１なる素数候補Ｎを生成する素数候補生成部と、
前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、
前記素数候補Ｎ及び前記乱数Ｒに対し、ＧＣＤ（２＾（２Ｒ）－１，Ｎ）＝１を満たすか否かを判定する第２の素数判定部と、を備えること
を特徴とする請求項２４から請求項２６のいずれか１項に記載の素数生成装置。
【請求項２９】
鍵発行サーバと、端末装置を備え、前記鍵発行サーバからＲＳＡ暗号の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行方法であって、
前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、
前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備えること
を特徴とする鍵発行方法。

【請求項３０】
鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行方法であって、
前記鍵発行サーバは、データを送信する送信部と、データを受信する受信部と、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、
前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、
前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備えること
を特徴とする鍵発行方法。
【請求項３１】
鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、
前記プログラムは、素数を含む前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵を格納する公開鍵格納ステップと、を前記端末装置に実行させ、
前記秘密鍵は発行識別子情報に基づいて生成された素数を含むこと
を特徴とするプログラム。
【請求項３２】
鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、
前記プログラムは、前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵証明書を格納する公開鍵証明書格納ステップと、を前記端末装置に実行させ、
前記秘密鍵は発行識別子情報に基づいて生成された素数を含むこと
を特徴とするプログラム。
【請求項３３】
鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバに実行させるプログラムであって、
前記プログラムは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成ステップと、を前記鍵発行サーバに実行させること
を特徴とするプログラム。
【請求項３４】
素数を生成する素数生成装置に実行させるプログラムであって、
前記プログラムは、発行識別子を生成する発行識別子生成ステップと、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、を前記素数生成装置に実行させること
を特徴とするプログラム。
【請求項３５】
請求項３１から請求項３４のいずれか１項に記載のプログラムを記録した媒体。

【書類名】明細書
【発明の名称】鍵発行システム、鍵発行装置、素数生成装置、鍵発行方法、素数生成方法及び記録媒体
【技術分野】
【０００１】
本発明は、素因数分解を安全性の根拠として実現する暗号などの情報セキュリティ技術に関する。
【背景技術】
【０００２】
近年、コンピュータ技術及び通信技術に基づくデータ通信が広く普及してきており、このデータ通信においては、秘密通信方式やデジタル署名方式が用いられる。ここで、秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行う方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、発信者の身元を証明したりする通信方式である。
【０００３】
１．公開鍵暗号方式
これらの秘密通信方式又はデジタル署名方式においては、公開鍵暗号方式とよばれる暗号方式が用いられる。公開鍵暗号方式を用いる秘密通信では、暗号化鍵と復号化鍵とが異なり、復号化鍵は秘密にするが、暗号化鍵は公開する。秘密にする復号化鍵を秘密鍵と呼び、公開する暗号化鍵を公開鍵と呼ぶ。通信相手が多数のとき、共通鍵暗号では通信相手間で鍵をもつ必要があるが、公開鍵暗号では通信相手が一つの固有の鍵をもつだけで通信可能になるため、通信相手が増えても、共通鍵暗号より鍵の数が少なくてよい。このように、公開鍵暗号は多数の通信相手と通信を行うのに適しており、不可欠な基盤技術である。
【０００４】
公開鍵暗号方式の１種であるＲＳＡ暗号方式では、整数の素因数分解問題を解くことが、計算量の上で困難であることを安全性の根拠としている。素因数分解問題とは、ｐ，ｑを素数とし、整数ｎ＝ｐ×ｑとするとき、整数ｎに対して、素数ｐ，ｑを求める問題である。ここで、×は通常の乗算である。一般にｐ，ｑが１０２４ビットの数のように大きい場合は、素因数分解問題が困難である。それにより、ＲＳＡ暗号方式の公開鍵から秘密鍵を求めることや、秘密鍵を持たないユーザが暗号文から平文を求めることが、困難になる。なお、素因数分解問題については、非特許文献１の１４４～１５１ページに詳しく述べられている。
【０００５】
（素因数分解問題を応用するＲＳＡ暗号方式）
素因数分解問題を応用するＲＳＡ暗号方式について説明する。
（１）鍵の生成
次に示すようにして公開鍵及び秘密鍵を計算する。
・ランダムに大きい素数ｐ，ｑを選択し、その積ｎ＝ｐ×ｑを計算する。
【０００６】
・（ｐ－１）及び（ｑ－１）の最小公倍数Ｌ＝ＬＣＭ（ｐ－１，ｑ－１）を計算する。
・Ｌと互いに素でＬより小さい自然数ｅをランダムに選ぶ。
　　１≦ｅ≦Ｌ－１、ＧＣＤ（ｅ，Ｌ）＝１
ここで、ＧＣＤ（ｅ，Ｌ）は、ｅとＬの最大公約数を示している。
・ｅ×ｄ＝１　ｍｏｄ　Ｌを満たすｄを計算する。ＧＣＤ（ｅ，Ｌ）＝１より、このようなｄは必ず存在する。このようにして、得られた整数ｅ及び整数ｎが、公開鍵である。また、整数ｄが、秘密鍵である。ここで、ｘ　ｍｏｄ　ｙは、ｘをｙで割った余りを示す。
【０００７】
（２）暗号文の生成

公開鍵である整数ｅ及び整数ｎを用いて、平文ｍに暗号演算を施して暗号文ｃを計算する。

ｃ＝ｍ＾ｅ　　ｍｏｄ　　ｎ

なお、この明細書において、演算子＾は、べき乗を示す。例えば、Ａ＾ｘは、　ｘ＞０のときはＡをｘ回乗じたものを示す。

【０００８】

（３）復号文の生成

秘密鍵である整数ｄを用いて、暗号文ｃに復号演算を施して復号文ｍ’を計算する。

ｍ’＝ｃ＾ｄ　　ｍｏｄ　　ｎ

なお、

ｍ’＝ｃ＾ｄ　　ｍｏｄ　　ｎ
＝（ｍ＾ｅ）＾ｄ　　ｍｏｄ　　ｎ
＝ｍ＾（ｅ×ｄ　　ｍｏｄ　　Ｌ）　　ｍｏｄ　　ｎ
＝ｍ＾１　　ｍｏｄ　　ｎ
＝ｍ　　ｍｏｄ　　ｎ

であるので、復号文ｍ’は、平文ｍと一致する。

【０００９】

また、ＲＳＡ暗号については、非特許文献２の１１０～１１３ページに詳しく説明されている。

上記に示した素因数分解を応用したＲＳＡ暗号における公開鍵の生成のステップにおいて、素数生成が行われる。素数生成については、非特許文献３の１４５～１５４ページに詳しく説明されている。素数生成方法には、確率的素数生成法と確定的素数生成方法がある。確率的素数生成法により生成される素数は、「素数である確率が高い」数であり、１００％素数であるとは限らない。一方、確定的素数生成方法は、確実に素数である数を生成する。確率的素数生成方法及び確定的素数生成方法については、非特許文献２に詳しく説明されている。以下では、確定的素数生成方法について説明する。

【００１０】

２．従来例１－確定的素数生成方法

確定的に素数を生成することができるＭａｕｒｅｒ法による確定的素数生成方法について説明する。ここで、Ｍａｕｒｅｒ法については、非特許文献３の１５２～１５３ページに詳しく説明されている。

前記確定的素数生成方法では、次に示すステップを繰り返すことにより、素数を生成する。あらかじめビットサイズｌｅｎｑの素数ｑが与えられている。

【００１１】

（ステップ１）（ｌｅｎｑ－１）ビットの乱数Ｒを選択する。なお、乱数Ｒの最上位ビットは、必ず１となるようにする。

（ステップ２）数Ｎを以下の式により計算する。

Ｎ＝２×ｑ×Ｒ＋１

（ステップ３）数Ｎが素数であるか否かを、次に示す第１判定及び第２判定がともに、成立する場合に、素数と判定する。他の場合に、素数でないと判定する。

【００１２】

（第１判定）　２＾（Ｎ－１）　＝１　　ｍｏｄ　　Ｎ
（第２判定）　ＧＣＤ（２＾（２Ｒ）－１、Ｎ）＝１

素数であると判定される場合には、数Ｎを素数として出力する。素数でないと判定される場合には、ステップ１へ戻って、素数が出力されるまで、処理を繰り返す。

ステップ３で述べられている判定方法は、Ｐｏｃｋｌｉｎｇｔｏｎの素数判定法とよばれ、非特許文献３の１４４ページに詳しく述べられている。Ｐｏｃｋｌｉｎｇｔｏｎ　の素数判定法では、Ｎ＝２×ｑ×Ｒ＋１のｑが素数であり、第１判定及び第２判定の結果が真であれば、必ず、Ｎが素数になる。そのため、確定的に素数であることを判定でき、確定的な素数生成が可能になる。

【００１３】
このようにして、Ｍａｕｒｅｒ法による確定的素数生成方法では、サイズｌｅｎｑの素数ｑを基にして、サイズ２×ｌｅｎｑの素数Ｎを生成する。従って、Ｍａｕｒｅｒ法による確定的素数生成方法を用いて所定長の素数を生成する場合には、前記所定長以下の素数の生成を繰り返し行う。例えば、５１２ビット長の素数を生成する場合には、あらかじめ与えられた８ビットの素数を基にして１６ビットの素数を生成する。次に、生成した１６ビットの素数を基にして３２ビットの素数を生成する。次に、生成した３２ビットの素数を基にして６４ビットの素数を生成する。以下同様の素数生成を繰り返して、５１２ビットの素数を生成する。

【００１４】
なお、前記第２判定を次の判定に代えてもよい。

（第３判定）　　２＾（２Ｒ）≠１　　ｍｏｄ　　Ｎ

上記第３判定方法は、非特許文献４に詳しく述べられている。以降、こちらの判定方法を使用していく。

３．複数の鍵発行サーバをもつ鍵発行システム

公開鍵暗号の鍵発行システムでは、ユーザが鍵を生成する場合や、鍵発行サーバによりユーザに鍵を発行する場合がある。鍵発行サーバにより鍵を発行する場合、ユーザに鍵を発行するサーバは一台であることが多い。しかし、ユーザが増加すると、上記のような素数生成方法は、複数回べき乗を行うことにより計算量が大きいため、計算時間が大きくなってくる。そこで、鍵発行サーバを複数もち、それぞれで鍵発行をすることにより、計算量の分散を図ることがある。

【特許文献１】特開２００３－５６４４号公報

【非特許文献１】岡本龍明、太田和夫共編、「暗号・ゼロ知識問題・数論」、共立出版、１９９０

【非特許文献２】岡本龍明、山本博資、”現代暗号”、産業図書（１９９７年）

【非特許文献３】Ａ．Ｊ．　Ｍｅｎｅｚｅｓ，　Ｐ．Ｃ．　ｖａｎ　Ｏｏｒｓｃｈｏｔ，　Ｓ．Ａ．　Ｖａｎｓｔｏｎｅ，　“Ｈａｎｄｂｏｏｋ　ｏｆ　ａｐｐｌｉｅｄ　ｃｒｙｐｔｏｇｒａｐｈｙ”，ＣＲＣ　Ｐｒｅｓｓ，　１９９７

【非特許文献４】岡本　栄司、「暗号理論入門」、共立出版、１９９３、２１ページ

【非特許文献５】Ｈｅｎｒｉ　Ｃｏｈｅｎ，　“Ａ　Ｃｏｕｒｓｅ　ｉｎ　Ｃｏｍｐｕｔａｔｉｏｎａｌ　Ａｌｇｅｂｒａｉｃ　Ｎｕｍｂｅｒ　Ｔｈｅｏｒｙ”，　ＧＴＭ　１３８，　Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ，　１９９３

【発明の開示】

【発明が解決しようとする課題】

【００１５】
鍵発行システムで鍵発行サーバを複数もつ場合、鍵発行がシステム全体で正しく行われていることを保証するため、鍵発行システム全体で統一的に同じ鍵発行方法を使用し、管理したいとの要望がある。また、鍵発行サーバでソフトウェアのバグなどにより、正しい鍵発行できない場合がある。システムから与えられた鍵発行方法を用いていることを検証機関により確認できれば、正しく鍵発行していることのある種の根拠となり、統一的な鍵発行を運用するための補助となる。また、鍵発行サーバが不正を働く可能性もあるため、この確認は、鍵発行したサーバ以外が行うのが望ましい。さらに、発行した秘密鍵を用いて確認を行うことは、検証機関が秘密鍵を暴露する可能性があり、望ましくない。したがって、発行した公開鍵を用いて確認できることが望ましい。

【００１６】
本発明は、公開鍵を用いて、正しく鍵発行しているかを確認できる鍵発行システムを提供することを目的とする。

【課題を解決するための手段】

【００１７】
上記目的を達成するために、請求項１における発明は、鍵発行サーバと、端末装置を備

え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムであって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備えることを特徴とする。

【００１８】

請求項２における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムであって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備えることを特徴とする。

【００１９】

請求項３における発明は、前記証明書発行サーバは、さらに、前記公開鍵が前記発行識別子に基づいた前記素数を用いて生成されているかを判定する鍵判定部を備えることを特徴とする。

請求項４における発明は、前記素数生成部は、前記発行識別子情報に基づいて２つの素数を生成することを特徴とする。

【００２０】

請求項５における発明は、前記素数生成部は、前記発行識別子情報ＩＤＩ及び０≦ｃ１，ｃ２＜ＩＤＩを満たす予め与えられた整数ｃ１，ｃ２に対して、Ｎ１＝ｃ１　ｍｏｄ　ＩＤＩ及びＮ２＝ｃ２　ｍｏｄ　ＩＤＩを満たす素数Ｎ１及びＮ２を生成することを特徴とする。

請求項６における発明は、前記鍵判定部は、前記素数Ｎ１及びＮ２の積である前記公開鍵ｎ（＝Ｎ１×Ｎ２）と前記整数ｃ１，ｃ２に対して、ｎ－ｃ１×ｃ２が発行識別子情報ＩＤＩで割り切れることを判定することを特徴とする。

【００２１】

請求項７における発明は、前記素数生成部は、第１素数ｑ、乱数Ｒ及び前記発行識別子情報ＩＤＩを用いてＮ＝２×Ｒ×ＩＤＩ×ｑ＋１で表される素数Ｎを生成することを特徴とする。

請求項８における発明は、前記素数生成部は、ｌｅｎビットの素数を生成し、ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、乱数Ｒを生成する乱数生成手段と、前記発行識別子情報ＩＤＩ、前記第１の素数ｑ及び前記乱数Ｒを用いて、Ｎ＝２×Ｒ×ＩＤＩ×ｑ＋１なる素数候補Ｎを生成する素数候補生成部と、前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、前記素数候補Ｎ及び前記乱数Ｒに対し、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する第２の素数判定部と、を備えることを特徴とする（ここで、ａ＾ｘはａのｘ乗を示す）。

【００２２】

請求項９における発明は、前記素数生成部は、ｌｅｎビットの素数を生成し、ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、乱数Ｒを生成する乱数生成手段と、前記発行識別子情報ＩＤＩ、前記第１の素数ｑ及び前記乱数Ｒを用いて、Ｎ＝２×Ｒ×ＩＤＩ×ｑ＋１なる素数候補Ｎを生成する素数候補生成部と、前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、前記素数候補Ｎ及び前記乱数Ｒに対し、ＧＣＤ（２＾（２Ｒ）－１

，Ｎ）＝１を満たすか否かを判定する第２の素数判定部と、を備えることを特徴とする（ここで、ＧＣＤ（Ｘ，Ｙ）はＸとＹの最大公約数を示す）。

【００２３】

請求項１０における発明は、前記鍵判定部は、前記公開鍵ｎに対して、ｎ－１が前記発行識別子情報ＩＤＩで割り切れることを判定することを特徴とする。

請求項１１における発明は、前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むことを特徴とする。

請求項１２における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置であって、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備え、前記秘密鍵は発行識別子情報に基づいて生成された複数の素数を含むことを特徴とする。

【００２４】

請求項１３における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置であって、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備え、前記秘密鍵は発行識別子情報に基づいて生成された複数の素数を含むことを特徴とする。

【００２５】

請求項１４における発明は、前記秘密鍵は前記発行識別子情報に基づいて生成された２つの素数を含むことを特徴とする。

請求項１５における発明は、前記２つの素数は、前記発行識別子情報ＩＤＩ及び０≦ｃ１，ｃ２＜ＩＤＩを満たす予め与えられた整数ｃ１，ｃ２に対して、Ｎ１＝ｃ１　ｍｏｄ　ＩＤＩ及びＮ２＝ｃ２　ｍｏｄ　ＩＤＩを満たす素数Ｎ１及びＮ２であることを特徴とする。

【００２６】

請求項１６における発明は、前記複数の素数は、第１素数ｑ、乱数Ｒ及び前記発行識別子情報ＩＤＩを用いてＮ＝２×Ｒ×ＩＤＩ×ｑ＋１で表されることを特徴とする。

請求項１７における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバであって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備えることを特徴とする。

【００２７】

請求項１８における発明は、前記素数生成部は、前記発行識別子情報に基づいて２つの素数を生成することを特徴とする。

請求項１９における発明は、前記素数生成部は、前記発行識別子情報ＩＤＩ及び０≦ｃ１，ｃ２＜ＩＤＩを満たす予め与えられた整数ｃ１，ｃ２に対して、Ｎ１＝ｃ１　ｍｏｄ　ＩＤＩ及びＮ２＝ｃ２　ｍｏｄ　ＩＤＩを満たす素数Ｎ１及びＮ２を生成することを特徴とする。

【００２８】

請求項２０における発明は、前記素数生成部は、第１素数ｑ、乱数Ｒ及び前記発行識別子情報ＩＤＩを用いてＮ＝２×Ｒ×ＩＤＩ×ｑ＋１で表される素数Ｎを生成することを特徴とする。

請求項２１における発明は、前記素数生成部は、１ｅｎビットの素数を生成し、１ｅｎｑ≧１ｅｎ／２を満たす１ｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、乱数Ｒを生成する乱数生成手段と、前記発行識別子情報ＩＤＩ、前記第１の素数ｑ及び前

記乱数Ｒを用いて、Ｎ＝２×Ｒ×ＩＤＩ×ｑ＋１なる素数候補Ｎを生成する素数候補生成部と、前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、前記素数候補Ｎ及び前記乱数Ｒに対し、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する第２の素数判定部と、を備えることを特徴とする。

【００２９】

請求項２２における発明は、前記素数生成部は、ｌｅｎビットの素数を生成し、ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、乱数Ｒを生成する乱数生成手段と、前記発行識別子情報ＩＤＩ、前記第１の素数ｑ及び前記乱数Ｒを用いて、Ｎ＝２×Ｒ×ＩＤＩ×ｑ＋１なる素数候補Ｎを生成する素数候補生成部と、前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、前記素数候補Ｎ及び前記乱数Ｒに対し、ＧＣＤ（２＾（２Ｒ）－１，Ｎ）＝１を満たすか否かを判定する第２の素数判定部と、を備えることを特徴とする。

【００３０】

請求項２３における発明は、前記発行識別子情報は、鍵発行サーバを識別する鍵発行サーバ識別子を含むことを特徴とする。

請求項２４における発明は、素数を生成する素数生成装置であって、前記素数生成装置は、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、を備えることを特徴とする。

【００３１】

請求項２５における発明は、前記素数生成部は、前記発行識別子情報ＩＤＩ及び０≦ｃ＜ＩＤＩを満たす予め与えられた整数ｃに対して、Ｎ＝ｃ　ｍｏｄ　ＩＤＩを満たす素数Ｎを生成することを特徴とする。

請求項２６における発明は、前記素数生成部は、第１素数ｑ、乱数Ｒ及び前記発行識別子情報ＩＤＩを用いてＮ＝２×Ｒ×ＩＤＩ×ｑ＋１で表される素数Ｎを生成することを特徴とする。

【００３２】

請求項２７における発明は、前記素数生成部は、ｌｅｎビットの素数を生成し、ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、乱数Ｒを生成する乱数生成手段と、前記発行識別子情報ＩＤＩ、前記第１の素数ｑ及び前記乱数Ｒを用いて、Ｎ＝２×Ｒ×ＩＤＩ×ｑ＋１なる素数候補Ｎを生成する素数候補生成部と、前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、前記素数候補Ｎ及び前記乱数Ｒに対し、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する第２の素数判定部と、を備えることを特徴とする。

【００３３】

請求項２８における発明は、前記素数生成部は、ｌｅｎビットの素数を生成し、ｌｅｎｑ≧ｌｅｎ／２を満たすｌｅｎｑビットの第１の素数ｑを生成する素数情報生成手段と、乱数Ｒを生成する乱数生成手段と、前記発行識別子情報ＩＤＩ、前記第１の素数ｑ及び前記乱数Ｒを用いて、Ｎ＝２×Ｒ×ＩＤＩ×ｑ＋１なる素数候補Ｎを生成する素数候補生成部と、前記素数候補Ｎに対し、２＾（Ｎ－１）＝１　ｍｏｄ　Ｎを満たすか否かを判定する第１の素数判定部と、前記素数候補Ｎ及び前記乱数Ｒに対し、ＧＣＤ（２＾（２Ｒ）－１，Ｎ）＝１を満たすか否かを判定する第２の素数判定部と、を備えることを特徴とする。

【００３４】

請求項２９における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバからＲＳＡ暗号の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行方法であって、前記鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を

備えることを特徴とする。

【００３５】

請求項３０における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行方法であって、前記鍵発行サーバは、データを送信する送信部と、データを受信する受信部と、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記証明書発行サーバは、前記公開鍵に対する前記公開鍵証明書を生成する公開鍵証明書生成部を備え、前記端末装置は、データを送信する送信部と、データを受信する受信部と、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵証明書を格納する公開鍵証明書格納部と、を備えることを特徴とする。

【００３６】

請求項３１における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、前記プログラムは、素数を含む前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵を格納する公開鍵格納ステップと、を前記端末装置に実行させ、前記秘密鍵は発行識別子情報に基づいて生成された素数を含むことを特徴とする。

【００３７】

請求項３２における発明は、鍵発行サーバと、証明書発行サーバと、端末装置を備え、前記鍵発行サーバが素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を生成し、前記証明書発行サーバが前記公開鍵に対する公開鍵証明書を生成し、前記鍵発行サーバが前記秘密鍵及び公開鍵証明書を前記端末装置へ送信する鍵発行システムにおける端末装置に実行させるプログラムであって、前記プログラムは、前記秘密鍵を格納する秘密鍵格納ステップと、前記公開鍵証明書を格納する公開鍵証明書格納ステップと、を前記端末装置に実行させ、前記秘密鍵は発行識別子情報に基づいて生成された素数を含むことを特徴とする。

【００３８】

請求項３３における発明は、鍵発行サーバと、端末装置を備え、前記鍵発行サーバから素因数分解問題を安全性の根拠とする暗号方式の秘密鍵及び公開鍵を前記端末装置へ送信する鍵発行システムにおける鍵発行サーバに実行させるプログラムであって、前記プログラムは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成ステップと、を前記鍵発行サーバに実行させることを特徴とする。

【００３９】

請求項３４における発明は、素数を生成する素数生成装置に実行させるプログラムであって、前記プログラムは、発行識別子を生成する発行識別子生成ステップと、前記発行識別子情報に基づいて素数を生成する素数生成ステップと、を前記素数生成装置に実行させることを特徴とする。

請求項３５における発明は、請求項３１から請求項３４のいずれか１項に記載のプログラムを記録した媒体である。

【発明の効果】

【００４０】

これらの構成によると、正しく鍵発行しているかを発行識別子情報ＩＤＩで割り切れるかをチェックすることで確認でき、その価値は大きい。

【発明を実施するための最良の形態】

【００４１】

（実施の形態１）

本発明に係る１の実施の形態としての素数生成装置１について、説明する。
図１は、実施の形態１における素数生成装置の構成を示す図である。
この素数生成装置１は、素数ｑ、ｑのビットサイズｌｅｎｑ、発行識別子情報ＩＤＩ及び識別子のビットサイズｌｅｎＩＤＩが与えられたとき、ｑのビットサイズｌｅｎｑの２倍のビットサイズ２×ｌｅｎｑをもつ素数を出力するものである。

【００４２】

＜素数生成装置１の構成＞
素数生成装置１は、乱数生成部１１と、素数候補生成部１２と、第１素数判定部１３と、第２素数判定部１４と、を備える。
乱数生成部１１は、ｌｅｎｑを用いて、（ｌｅｎｑ－ｌｅｎＩＤＩ－１）ビットの乱数Ｒ’を生成する。ここで、乱数Ｒ’の最上位ビットは１とする。

【００４３】

素数候補生成部１２は、ｑ及びＲ’を用いて、以下の式を満たすＲとＮを生成する。

$$R = IDI \times R'$$

$$N = 2 \times R \times q + 1$$

第１素数判定部１３は、Ｎを用いて、以下の式の成立を判定する。

【００４４】

$$2^{(N-1)} = 1 \mod N \quad (eq1)$$

ここで、２＾（Ｎ－１）は、２のＮ－１乗を示している。
第２素数判定部１４は、ＮとＲを用いて、以下の式を満たすか否かを判定する。

$$2^{(2R)} \neq 1 \mod N \quad (eq2)$$

＜素数生成装置１の動作＞
以下に素数生成装置１の動作を示す。図２にこの動作のフローチャートを示す。

【００４５】

ステップＳ１０１：乱数生成部１１は、（ｌｅｎｑ－ｌｅｎＩＤＩ－１）ビットの乱数Ｒ’を生成する。ここで、Ｒ’の最上位ビットは１とする。
ステップＳ１０２：素数候補生成部１２は、ＲとＮを計算する。
ステップＳ１０３：第１素数判定部１３は、２＾（Ｎ－１）　＝　１　ｍｏｄ　Ｎの成立を判定する。この式が成立する場合は次のＳ１０４ステップへ。成立しない場合はステップＳ１０１へ。

【００４６】

ステップＳ１０４：第２素数判定部１４は、２＾（２Ｒ）　≠　１　ｍｏｄ　Ｎを満たすか否かを判定する。この式が成立する場合はＮを出力し、終了する。成立しない場合は、ステップＳ１０１へ。

＜実施の形態１の効果＞
生成された素数Ｎに対して、Ｎ－１は必ず発行識別子情報ＩＤＩで割り切れる。なぜなら、Ｎ－１＝２×ｑ×Ｒ＝２×ｑ×ＩＤＩ×Ｒ’が成り立つためである。したがって、生成された素数が発行識別子情報ＩＤＩで割り切れるか否かで、素数生成装置１を用いて素数が生成されたかを確認することができる。

【００４７】

なお、ＩＤＩのビットサイズがｌｅｎＩＤＩであり、Ｒ’のビットサイズが（ｌｅｎｑ－ｌｅｎＩＤＩ－１）であるため、ほとんどのＮ＝２×ｑ×ＩＤＩ×Ｒ’＋１のビットサイズは、２×ｌｅｎｑとなる。ここで、ｑやＩＤＩなどの値によっては、ビットサイズが２×ｌｅｎｑ－１となる場合がある。その場合は、素数候補生成部１２で、Ｒ’に２を掛けて、それを新たにＲ’とみなすことにより、Ｎのビットサイズを２×ｌｅｎｑになるように設定する。

【００４８】

（実施の形態２）
本発明に係る２の実施の形態としての素数生成装置２について、説明する。
図３は、実施の形態２における素数生成装置の構成を示す図である。

この素数生成装置２は、素数ｑ、ｑのビットサイズｌｅｎｑ、発行識別子情報ＩＤＩ、発行識別子情報のビットサイズｌｅｎＩＤＩ及び検証値ｃが与えられたとき、ｑのビットサイズｌｅｎｑの２倍のビットサイズ２×ｌｅｎｑをもつ素数を出力するものである。ここで、ＩＤＩは奇数とする。

【００４９】

＜素数生成装置２の構成＞

素数生成装置２は、実施形態１の素数生成装置１と同様の乱数生成部１１と、第１素数判定部１３と、第２素数判定部１４と、素数生成装置２と異なる素数候補生成部２２と、を備える。

素数候補生成部２２は、ｑ及びＲ’を用いて、以下の式を満たすＲとＮを生成する。

【００５０】

$$R = IDI \times R'$$

$$N = 2 \times (R + w) \times q + 1$$

ここで、ｗは$2 \times w \times q + 1 = c \mod IDI$，$0 \leqq w < IDI$を満たす数である。ｗは、$w = (c - 1) \times m \mod IDI$を計算することにより求める。ｍは$(2 \times q) \times m = 1 \mod IDI$を満たす数である。ＩＤＩが奇数、すなわち、ＧＣＤ（ＩＤＩ，２）＝１であり、ＩＤＩ＜ｑであるため、ｍは計算可能である。計算方法については、非特許文献５が詳しい。

【００５１】

＜素数生成装置２の動作＞

以下に素数生成装置２の動作を示す。図４にこの動作のフローチャートを示す。

ステップＳ２０１：乱数生成部１１は、（ｌｅｎｑ－ｌｅｎＩＤＩ－１）ビットの乱数Ｒ’を生成する。ここで、Ｒ’の最上位ビットは１とする。

【００５２】

ステップＳ２０２：素数候補生成部２２は、ＲとＮを計算する。

ステップＳ２０３：第１素数判定部１３は、$2^{(N-1)} = 1 \mod N$の成立を判定する。この式が成立する場合は次のステップＳ２０４へ。成立しない場合はステップＳ２０１へ。

ステップＳ２０４：第２素数判定部１４は、$2^{(2R)} \neq 1 \mod N$の成立を判定する。この式が成立する場合はＮを出力し、終了する。成立しない場合は、ステップＳ２０１へ。

【００５３】

＜実施の形態２の効果＞

生成された素数Ｎに対して、Ｎ－ｃは必ず発行識別子情報ＩＤＩで割り切れる。なぜなら、$N - c = 2 \times q \times R + 1 - c = 2 \times q \times (IDI \times R' + w) + 1 - c$であり、$2 \times q \times w + 1 = c \mod IDI$が成り立つためである。したがって、生成された素数Ｎに対し、Ｎ－ｃが発行識別子情報ＩＤＩで割り切れるか否かで、素数生成装置２を用いて素数が生成されたかを確認することができる。

【００５４】

なお、ＩＤＩのビットサイズがｌｅｎＩＤＩであり、Ｒ’のビットサイズが（ｌｅｎｑ－ｌｅｎＩＤＩ－１）であるため、ほとんどの$N = 2 \times q \times (IDI \times R' + w) + 1$のビットサイズは、２×ｌｅｎｑとなる。ここで、ｑやＩＤＩなどの値によっては、ビットサイズが２×ｌｅｎｑ－１となる場合がある。その場合は、素数候補生成部１２で、Ｒ’に２を掛けて、それを新たにＲ’とみなすことにより、Ｎのビットサイズを２×ｌｅｎｑになるように設定する。

【００５５】

（実施の形態３）

本発明に係る３の実施の形態としての鍵発行システム３について、説明する。

図５は、実施の形態３における鍵発行システム３の構成を示す図である。本システムは、鍵発行サーバＡ３１、Ｂ３２、Ｃ３３と、証明書発行サーバ３４と、端末装置３５１、３

５２、３５３、．．．、３５ｎから構成される。ｎは自然数であり、例えば１０００である。この場合、端末装置が１０００台存在することになる。

＜鍵発行サーバＡ３１、Ｂ３２、Ｃ３３の構成＞

鍵発行サーバＡ３１、Ｂ３２、Ｃ３３は同じ構成であるため、以下では代表して鍵発行サーバＡ３１の構成を示す。鍵発行サーバＡ３１、Ｂ３２、Ｃ３３にはそれぞれ、予め識別子：ＳＩＤＡ、ＳＩＤＢ、ＳＩＤＣが与えられている。

【００５６】

鍵発行サーバＡ３１は、予め与えられた検証値ｃ１，ｃ２を用いてＲＳＡ暗号における秘密鍵及び公開鍵を生成し、公開鍵を証明書発行サーバへ送信し、公開鍵証明書を受信した後、端末装置へ送信する。

鍵発行サーバＡ３１は、送信部３１０１と、受信部３１０２と、識別子生成部３１０３、識別子格納部３１０４と、素数生成部３１０５と、秘密鍵判定部３１０６と、鍵生成部３１０７と、秘密鍵格納部３１０８と、公開鍵格納部３１０９と、証明書格納部３１１０を備える（図６参照）。

【００５７】

送信部３１０１は、端末装置３５ｉ（ｉ＝１～ｎ）へ生成した秘密鍵及び公開鍵を、証明書発行サーバ３４へ公開鍵を送信する。

受信部３１０２は、端末装置３５ｉから鍵生成要求情報を、証明書発行サーバ３４から公開鍵証明書Ｃｅｒｔを受信する。公開鍵証明書については、証明書発行サーバ３４の構成の説明で述べる。

【００５８】

識別子生成部３１０３は、端末装置３５ｉ用に素数の発行識別子情報ＩＤＩを生成し、識別子格納部３１０４に格納する。発行識別子情報ＩＤＩは、予め与えられた各鍵発行サーバに対応する識別子：ＳＩＤ（Ａ３１はＳＩＤＡ、Ｂ３２はＳＩＤＢ、Ｃ３３はＳＩＤＣ）と発行識別子：ＰＩＤからなる。例えば、ＩＤＩ＝ＳＩＤ｜｜ＰＩＤとする。ここで、｜｜はビットまたはバイト連結である。発行識別子は例えば、１から発行順に数字を割り当て、発行するたびにインクリメントする。

【００５９】

識別子格納部３１０４は、素数の発行識別子情報ＩＤＩを格納する。

素数生成部３１０５は、５１２ビット素数を生成する。なお、ここでは鍵長が１０２４ビットのＲＳＡを想定しているため、５１２ビット素数を生成するとしたが、鍵長をｌｅｎビットとして、ｌｅｎ／２ビットの素数を生成するとしてもよい。

（素数生成部３１０５の構成及び動作）

素数生成部３１０５は、第１の素数生成部３１０５１と、第２の素数生成部３１０５２と、を備える（図７参照）。

【００６０】

第１の素数生成部３１０５１は、２５６ビットの素数ｑを生成する。素数の生成方法は従来の方法を用いる。従来の方法については、特許文献１及び非特許文献３が詳しい。

第２の素数生成部３１０５２は、２５６ビット素数ｑと、ｑのビットサイズ２５６と、発行識別子情報ＩＤＩ及び、予め与えられた検証値ｃ１またはｃ２を用いて、５１２ビットの素数Ｎを生成する。第２の素数生成部３１０５２は、実施形態２の素数生成装置２を用いて、素数Ｎを生成する。

【００６１】

秘密鍵判定部３１０６は、２回の素数生成部３１０５の処理を実行して出力された素数ｐ１とｐ２が一致しているかを比較する。

鍵生成部３１０７は、秘密鍵格納部３１０８に格納されている秘密鍵ｐ１、ｐ２の積ｎ＝ｐ１×ｐ２を計算し、さらに、乱数ｅを生成し、それらのｎとｅの組ＰＫ＝（ｎ，ｅ）を公開鍵とする。

【００６２】

その後、ｅ×ｄ＝１　ｍｏｄ　Ｌを満たすｄを計算し秘密鍵とする。ここで、Ｌ＝ＬＣＭ（ｐ１－１，ｐ２－１）である。ＬＣＭ（ｐ１－１，ｐ２－１）はｐ１－１とｐ２－１の最小公倍数を示す。

秘密鍵格納部３１０８は、素数生成部３１０５で生成した２つの素数ｐ１、ｐ２と鍵生成部で作成したｄの組ＳＫ＝（ｐ１，ｐ２，ｄ）を秘密鍵として格納する。

【００６３】

公開鍵格納部３１０９は、鍵生成部３１０７で生成した公開鍵ＰＫを格納する。

証明書格納部３１１０は、証明書発行サーバ３４が送信した公開鍵証明書Ｃｅｒｔを格納する。

＜鍵発行サーバＡ３１、Ｂ３２、Ｃ３３の動作＞

鍵発行サーバＡ３１、Ｂ３２、Ｃ３３の動作は同様であるため、以下に代表して鍵発行サーバＡ３１の動作を示す。ここでは、端末装置３５ｉ（ｉは１からｎのいずれかの数）から鍵発行依頼情報が送信された場合の動作を示している。図８にこの動作のフローチャートを示す。

【００６４】

ステップＳ３０１：受信部３１２は、端末装置３５ｉより送信された鍵発行依頼情報を受信する。

ステップＳ３０２：識別子生成部３１３は、発行識別子情報：ＩＤＩを生成し、識別子格納部２１４に格納する。

ステップＳ３０３：素数生成部３１５は、予め与えられた検証値ｃ１を用いて、素数ｐ１を生成する。

【００６５】

ステップＳ３０４：素数生成部３１５は、予め与えられた検証値ｃ２を用いて、素数ｐ２を生成する。

ステップＳ３０５：秘密鍵判定部３１６は、素数ｐ１とｐ２がｐ１＝ｐ２を満たすかを判定する。ｐ１＝ｐ２の場合は、ステップＳ３０４へ。それ以外は、秘密鍵格納部３１８に格納する。次のステップＳ３０６へ。

【００６６】

ステップＳ３０６：鍵生成部３１７は、ｎ＝ｐ１×ｐ２を計算する。また、鍵生成部３１７は、乱数ｅを生成し、ｎとｅの組ＰＫ＝（ｎ，ｅ）を公開鍵として公開鍵格納部３１９に格納する。さらに、鍵生成部３１７は、ｅ×ｄ＝１　ｍｏｄ　Ｌを満たすｄを計算し、ｐ１、ｐ２とｄの組ＳＫ＝（ｐ１，ｐ２，ｄ）を秘密鍵として秘密鍵格納部３１８に格納する。

【００６７】

ステップＳ３０７：送信部３１１は、公開鍵格納部３１９に格納されている公開鍵ＰＫ及び識別子格納部３１４に格納されている発行識別子情報ＩＤＩを証明書発行サーバ３４へ送信する。

ステップＳ３０８：受信部３１２は、証明書発行サーバ３４より送信された公開鍵証明書Ｃｅｒｔを受信する。

【００６８】

ステップＳ３０９：送信部３１１は、秘密鍵格納部３１８に格納されている秘密鍵ＳＫ＝（ｐ１，ｐ２，ｄ）と、公開鍵証明書Ｃｅｒｔを端末装置３５ｉへ送信し、終了する。

＜証明書発行サーバ３４の構成＞

証明書発行サーバ３４は、送信部３４１と、受信部３４２と、秘密鍵格納部３４３と、発行公開鍵確認部３４４と、発行公開鍵格納部３４５と、発行識別子情報格納部３４６と、公開鍵証明書生成部３４７と、公開鍵証明書格納部３４８と、を備える（図９参照）。

【００６９】

送信部３４１は、証明書Ｃｅｒｔを鍵発行サーバＡ３１、Ｂ３２または、Ｃ３３へ送信する。

受信部３４２は、鍵発行サーバＡ３１、Ｂ３２または、Ｃ３３から公開鍵ｎ、ｅを受信

する。
秘密鍵格納部３４３は、証明書発行サーバ３４の秘密鍵ＳＫＣＡを格納する。
【００７０】
発行公開鍵確認部３４４は、鍵発行サーバＡ３１、Ｂ３２またはＣ３３から受信した公開鍵ＰＫ＝（ｎ，ｅ）と発行識別子情報ＩＤＩを用いて、公開鍵ＰＫ＝（ｎ，ｅ）が発行識別子情報ＩＤＩを用いて生成されたかを確認する。具体的には、検証値ｃ１及びｃ２を用いて、ｎ－ｃ１×ｃ２がＩＤＩで割り切れるかでチェックする。割り切れる場合は、公開鍵ＰＫ＝（ｎ，ｅ）が発行識別子情報ＩＤＩで生成されたと判断し、それ以外は発行識別子情報ＩＤＩで生成されていないと判断する。
【００７１】
発行公開鍵格納部３４５は、鍵発行サーバＡ３１、Ｂ３２またはＣ３３から受信した公開鍵ＰＫ＝（ｎ，ｅ）を格納する。
発行識別子情報格納部３４６は、鍵発行サーバＡ３１、Ｂ３２またはＣ３３から受信した発行識別子情報ＩＤＩを格納する。
公開鍵証明書生成部３４７は、公開鍵ＰＫと発行識別子情報ＩＤＩに対する公開鍵証明書Ｃｅｒｔを、秘密鍵格納部３４３に格納されている秘密鍵ＳＫＣＡを用いて生成する。具体的には、例えば、Ｃｅｒｔ＝ｎ｜｜ｅ｜｜ＩＤＩ｜｜Ｓｉｇ（ＳＫＣＡ，ｎ｜｜ｅ｜｜ＩＤＩ）とする。ここで、Ｓｉｇ（Ｋ，Ｄ）はデータＤに対する鍵Ｋを用いたときの署名データである。また、｜｜はビットまたはバイトの連結である。
【００７２】
公開鍵証明書格納部３４８は、公開鍵証明書Ｃｅｒｔを格納する。
＜証明書発行サーバ３４の動作＞
以下に証明書発行サーバ３４の動作を示す。ここでは、証明書を発行する先を鍵発行サーバＡ３１として動作を示す。なお、他の鍵発行サーバ（Ｂ３２、Ｃ３３）を発行先の場合も同様の動作を行う。図１０にこの動作のフローチャートを示す。
【００７３】
ステップＳ４０１：受信部３４２は、鍵発行サーバＡ３１から送信された公開鍵ＰＫ＝（ｎ，ｅ）と発行識別子情報ＩＤＩを受信する。
ステップＳ４０２：発行公開鍵確認部３４４は、公開鍵ＰＫ＝（ｎ，ｅ）が発行識別子情報ＩＤＩを用いて生成されたかを確認する。公開鍵ＰＫ＝（ｎ，ｅ）が発行識別子情報ＩＤＩで生成されていると判断した場合は、次のステップＳ４０３へ。それ以外は、システムを終了する。
【００７４】
ステップＳ４０３：発行公開鍵格納部３４５は、公開鍵ＰＫ＝（ｎ，ｅ）を、発行識別子情報格納部３４６は、発行識別子情報ＩＤＩをそれぞれ格納する。
ステップＳ４０４：公開鍵証明書生成部３４７は、公開鍵ＰＫ＝（ｎ，ｅ）と発行識別子情報ＩＤＩに対する公開鍵証明書Ｃｅｒｔを生成し、公開鍵証明書格納部３４８に格納する。
【００７５】
ステップＳ４０５：送信部３４１は、公開鍵証明書格納部３４８に格納されている公開鍵証明書Ｃｅｒｔを鍵発行Ａ３１へ送信し、終了する。
＜端末装置３５ｉ（ｉ＝１～ｎ）の構成＞
端末装置３５１、３５２、３５３、．．．、３５ｎはそれぞれ、同じ構成をしているため、以下では代表して、端末装置３５ｉの構成を示す。
【００７６】
端末装置３５ｉは、送信部３５ｉ１と、受信部３５ｉ２と、秘密鍵格納部３５ｉ３と、公開鍵格納部３５ｉ４と、発行識別子情報格納部３５ｉ５と、を備える（図１１参照）。
送信部３５ｉ１は、鍵発行依頼情報を鍵発行サーバＡ３１、Ｂ３２、Ｃ３３のいずれかへ送信する。鍵発行依頼情報は、例えば、端末装置３５ｉを示す識別子情報などである。
受信部３５ｉ２は、鍵発行サーバＡ３１，Ｂ３２，Ｃ３３のいずれかから送信された秘

密鍵ＳＫ＝（ｐ１，ｐ２，ｄ）、公開鍵ＰＫ＝（ｎ，ｅ）と、発行識別子情報ＩＤＩを受信する。

【００７７】

秘密鍵格納部３５ｉ３は、秘密鍵ＳＫ＝（ｐ１，ｐ２，ｄ）を格納する。

公開鍵証明書格納部３５ｉ４は、公開鍵証明書Ｃｅｒｔを格納する。

＜端末装置３５ｉの動作＞

以下に端末装置３５ｉの動作を示す。ここでは、鍵発行サーバＡ３１に鍵発行を依頼する場合の動作を示している。図１２にこの動作のフローチャートを示す。

【００７８】

ステップＳ５０１：送信部３５ｉ１は、鍵発行依頼情報を鍵発行サーバＡ３１へ送信する。

ステップＳ５０２：受信部３５ｉ２は、鍵発行サーバＡ３１より送信された秘密鍵ＳＫ＝（ｐ１，ｐ２，ｄ）、公開鍵証明書Ｃｅｒｔを受信する。

ステップＳ５０３：秘密鍵格納部３５ｉ３は、秘密鍵ＳＫ＝（ｐ１，ｐ２，ｄ）を格納する。

【００７９】

ステップＳ５０４：公開鍵証明書格納部３５ｉ４は、公開鍵証明書Ｃｅｒｔを格納し、終了する。

＜鍵発行システム３の動作＞

以下に鍵発行システム３の動作を示す。以下では、鍵発行サーバＡ３１が端末装置３５ｉに鍵を発行するときの動作を示す。端末装置３５ｉは、まず、鍵発行依頼情報を鍵発行サーバＡ３１へ送信する。鍵発行サーバＡ３１は、鍵発行依頼情報を受信した後、発行識別子情報ＩＤＩを作成する。その後、鍵発行サーバＡ３１は秘密鍵ＳＫ＝（ｐ１，ｐ２、ｄ）、公開鍵証明書ＰＫ＝（ｎ，ｅ）を生成する。さらに、鍵発行サーバＡ３１は、公開鍵ＰＫ＝（ｎ，ｅ）と発行識別子情報ＩＤＩを証明書発行サーバ３４へ送信する。証明書発行サーバ３４は、公開鍵ＰＫに対応する秘密鍵ＳＫに含まれる素数ｐ１、ｐ２が発行識別子情報ＩＤＩを用いて生成されているかを判定する。証明書発行サーバ３４は、判定結果が肯定的な場合に、公開鍵ＰＫに対する公開鍵証明書Ｃｅｒｔを生成し、公開鍵証明書Ｃｅｒｔを鍵発行サーバＡ３１へ送信する。鍵発行サーバＡ３１は、秘密鍵ＳＫ＝（ｐ１，ｐ２，ｄ）と公開鍵証明書Ｃｅｒｔを端末装置３５ｉへ送信する。端末装置３５ｉは、秘密鍵ＳＫ、公開鍵証明書Ｃｅｒｔを格納し、システムを終了する。

【００８０】

＜実施の形態３の効果＞

証明書発行サーバは、鍵発行サーバが正しく発行識別子情報ＩＤＩを用いて生成しているかを確認することができる。なぜなら、秘密鍵である素数ｐ１、ｐ２はそれぞれ、素数ｑ１、ｑ２、乱数Ｒ１’、Ｒ２’、発行識別子情報ＩＤＩに対して、ｐ１＝２×ｑ１×（ＩＤＩ×Ｒ１’＋ｒ１’）＋１＝ｃ１　ｍｏｄ　ＩＤＩ、ｐ２＝２×ｑ２×（ＩＤＩ×Ｒ２’＋ｒ２’）＋１＝ｃ２　ｍｏｄ　ＩＤＩを満たすため、

ｎ＝ｐ１×ｐ２＝（２×ｑ１×ＩＤＩ×Ｒ１’＋１）×（２×ｑ２×ＩＤＩ×Ｒ２’＋１）

＝ｃ１×ｃ２　ｍｏｄ　ＩＤＩ

となる。そのため、ｎ－ｃ１×ｃ２はＩＤＩで割り切れるため、ｎ－ｃ１×ｃ２がＩＤＩで割り切れることを確認することで、素数ｐ１、ｐ２が正しく発行識別子情報ＩＤＩを用いて生成しているかを確認することができる。

【００８１】

なお、端末がその端末がもつ秘密鍵を用いて、不正を働いたとき、以下の確認方法により、秘密鍵より不正を働いた端末の情報を得ることができる。不正を働いた端末の秘密鍵ｐ１，ｐ２が判明したとする。また、不正の追跡者は、発行識別子情報と端末の対応表と持っているとする。ｐ１－ｃ１，ｐ２－ｃ２は共に発行識別子情報ＩＤＩで割り切れる。そのため、ＧＣＤ（ｐ１－ｃ１，ｐ２－ｃ２）は発行識別子情報で割り切れる。したがっ

て、ＧＣＤ（ｐ１－ｃ１，ｐ２－ｃ２）の素因数を調べることにより、不正の追跡者は、取りうる発行識別子情報を限定でき、発行識別子情報を知る、すなわち、端末を特定するための助けとなる。

【００８２】

（変形例）

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。例えば、以下のような場合も本発明に含まれる。

（１）先にも述べたが、実施の形態３における、生成する秘密鍵である素数のビットサイズは５１２に限らない。１０２４であっても、２０４８であってもよい。また、素数情報生成部で生成する素数も同様に２５６ビットに限らない。

【００８３】

（２）実施の形態３の鍵発行サーバは、素数生成装置２を使用しているが、素数生成装置１を使用してもよい。その場合は、証明書発行サーバはｎ－１がＩＤＩで割り切れることを確認する。

（３）実施の形態１、または２の素数生成装置を素数生成手段として用いて、整数ｌｅｎと発行識別子情報ＩＤＩを入力とし、ｌｅｎビットの素数を出力する素数生成装置としてもよい。

【００８４】

（４）鍵発行サーバは３台以外の何台であってもよい。

【産業上の利用可能性】

【００８５】

これらの構成によると、正しく鍵発行しているかを発行識別子情報ＩＤＩで割り切れるかをチェックすることで確認できる。

【図面の簡単な説明】

【００８６】

【図１】本発明に係る１個の実施の形態としての素数生成装置１の構成を示すブロック図

【図２】素数生成装置１の動作を示すフローチャート

【図３】本発明に係る１個の実施の形態としての素数生成装置２の構成を示すブロック図

【図４】素数生成装置２の動作を示すフローチャート

【図５】本発明に係る１個の実施の形態としての鍵発行システム３の構成を示すブロック図

【図６】鍵発行サーバＡ３１の構成を示す図

【図７】素数生成部３１０５の構成を示す図

【図８】鍵発行サーバＡ３１の動作を示すフローチャート

【図９】証明書発行サーバ３４の構成を示す図

【図１０】証明書発行サーバ３４の動作を示すフローチャート

【図１１】端末装置３５ｉの構成を示す図

【図１２】端末装置３５ｉの動作を示すフローチャート

【符号の説明】

【００８７】

１、２　素数生成装置

１１　乱数生成部

１２、２２　素数候補生成部

１３　第１素数判定部

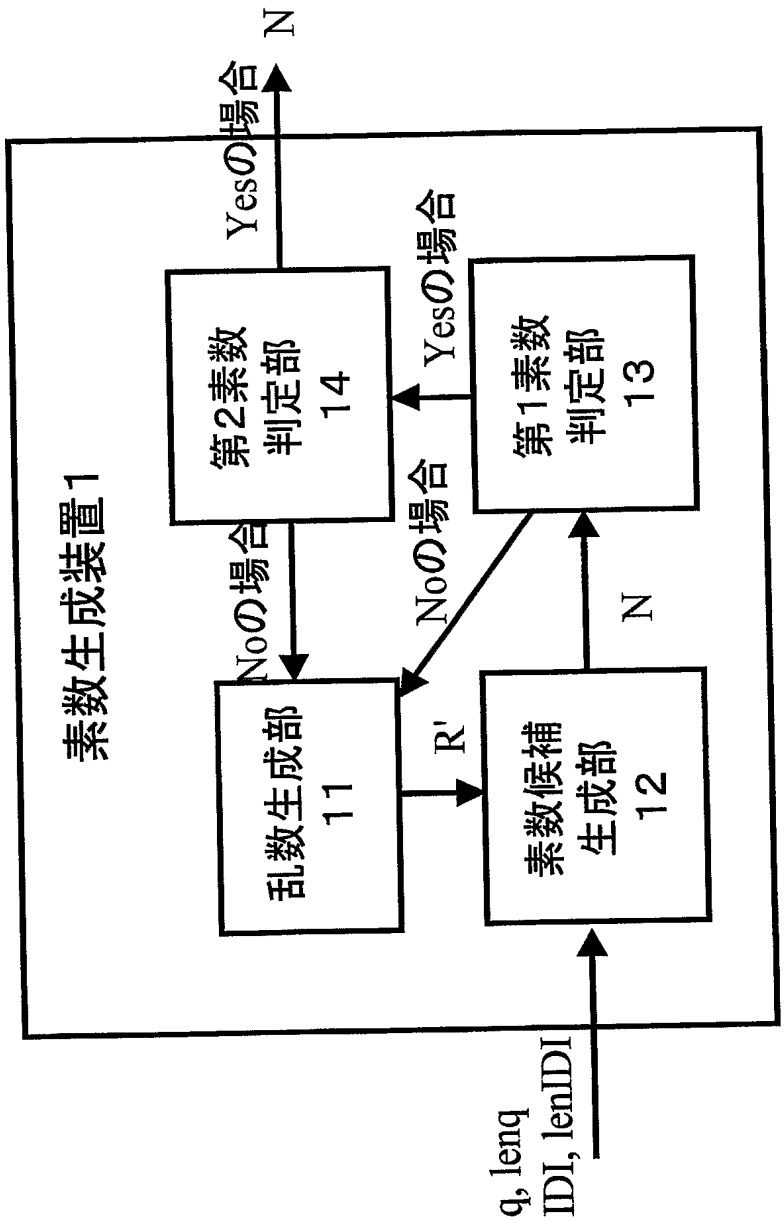
１４　第２素数判定部

３　鍵発行システム

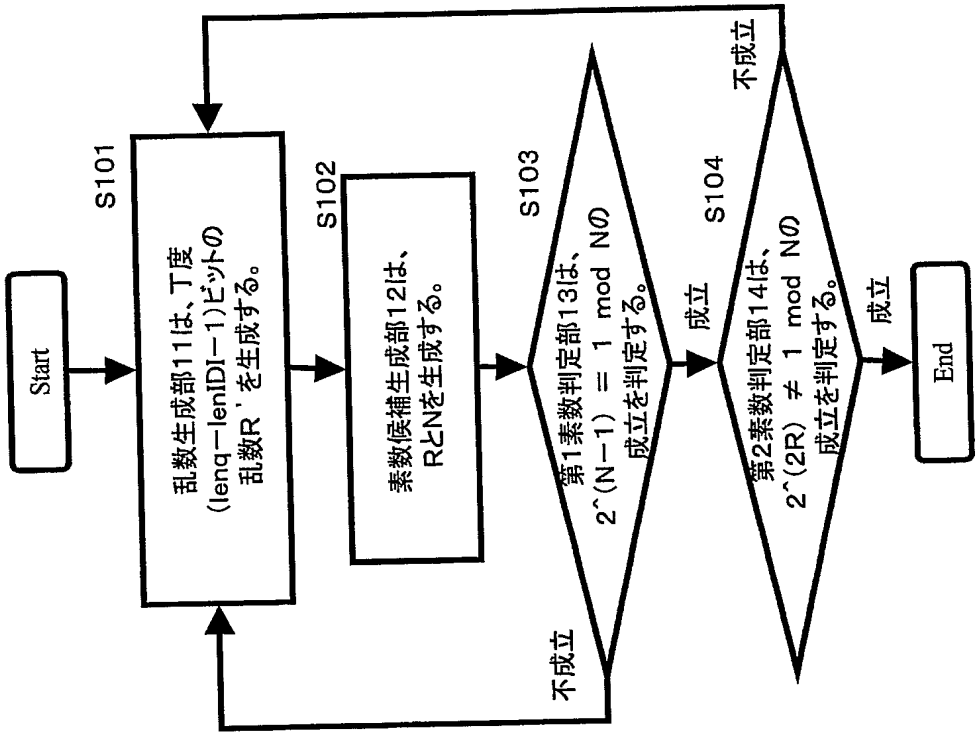
３１　鍵発行サーバＡ

３１０１、３４１、３５ｉ１　送信部
３１０２、３４２、３５ｉ２　受信部
３１０３　識別子生成部
３１０４　識別子格納部
３１０５　素数生成部
３１０５１　第１の素数生成部
３１０５２　第２の素数生成部
３１０６　秘密鍵判定部
３１０７　鍵生成部
３１０８、３４３、３５ｉ３　秘密鍵格納部
３１０９　公開鍵格納部
３１１０、３４７、３５ｉ４　公開鍵証明書格納部
３２　鍵発行サーバＢ
３３　鍵発行サーバＣ
３４　証明書発行サーバ
３４４　発行公開鍵確認部
３４５　発行公開鍵格納部
３４６　公開鍵証明書生成部
３５ｉ（ｉ＝１～ｎ）　端末装置

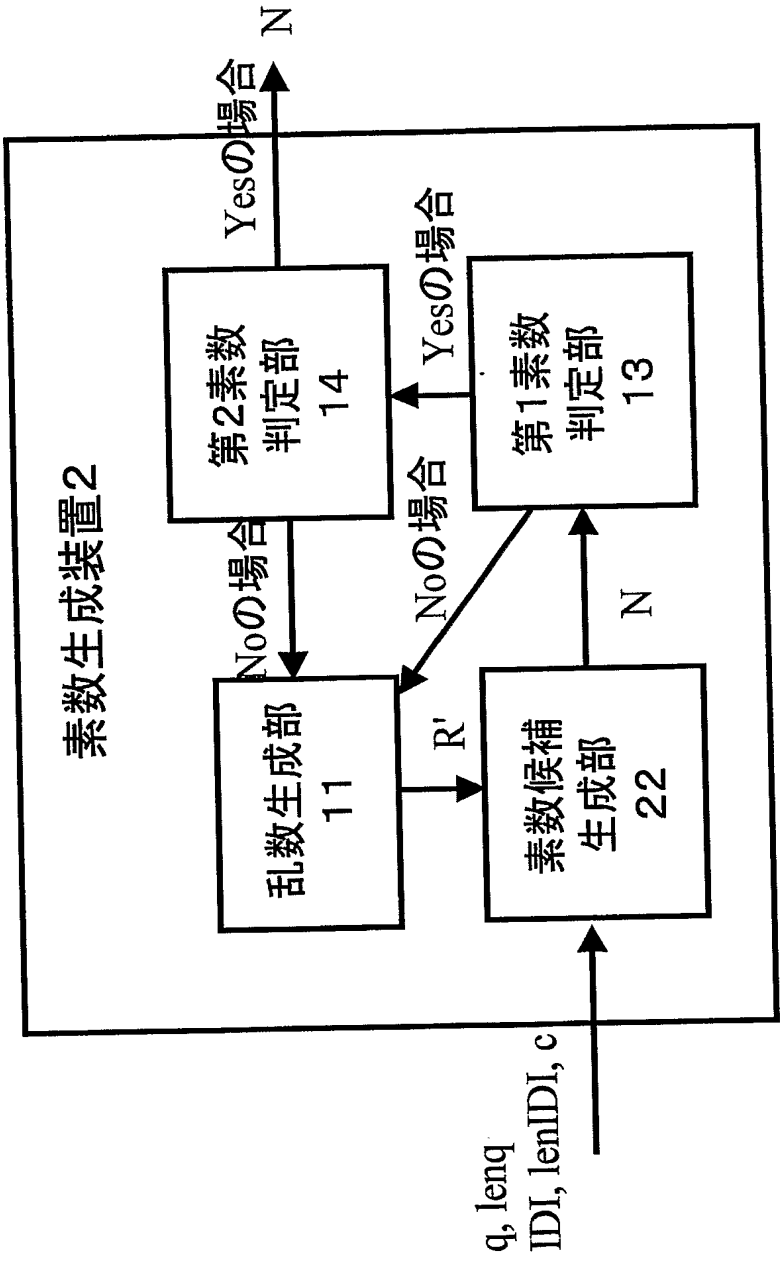
【書類名】図面
【図１】


素数生成装置1
乱数生成部
11
R'
素数候補
生成部
12
N
第1素数
判定部
13
Yesの場合
第2素数
判定部
14
Noの場合
Yesの場合
N
Noの場合
q, lenq
IDI, lenIDI

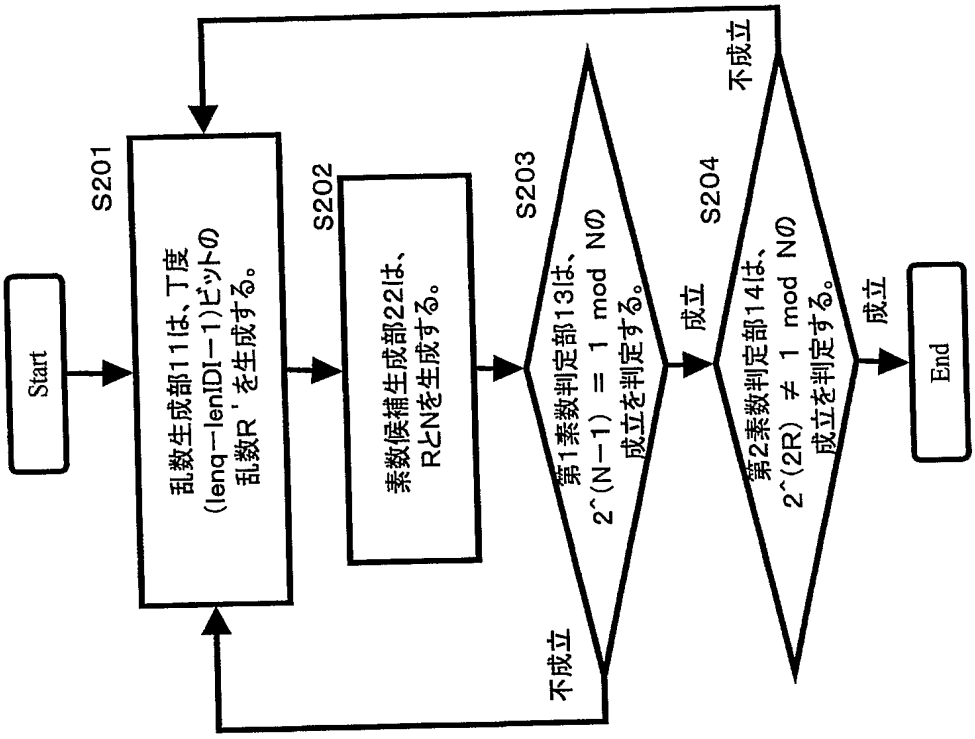
【図２】


Start
S101
乱数生成部11は、T度
(lenq－lenIDI－1)ビットの
乱数R'を生成する。
S102
素数候補生成部12は、
RとNを生成する。
S103
第1素数判定部13は、
2^(N－1) ＝ 1 mod Nの
成立を判定する。
不成立
成立
S104
第2素数判定部14は、
2^(2R) ≠ 1 mod Nの
成立を判定する。
不成立
成立
End

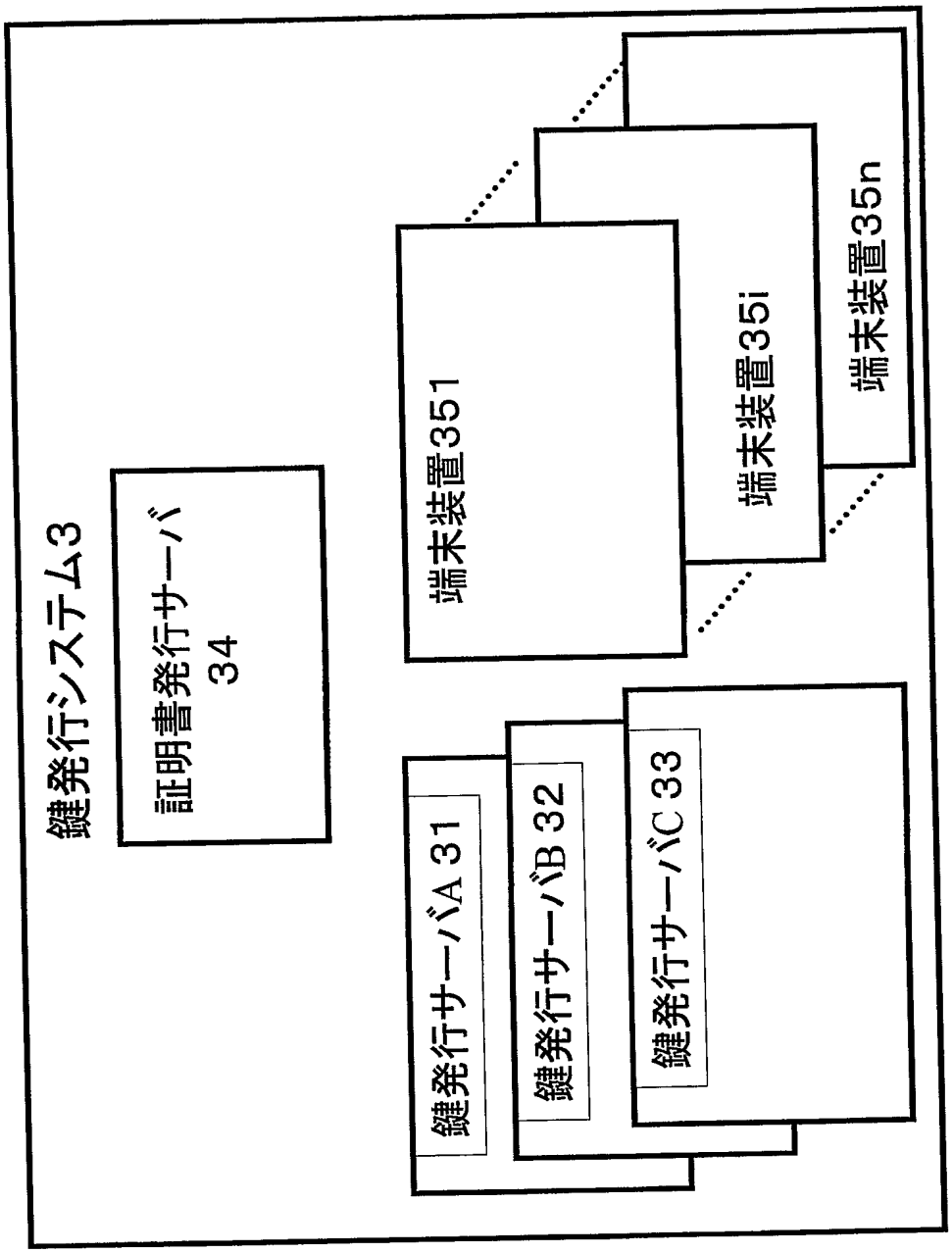
【図３】


素数生成装置2
乱数生成部
11
R'
素数候補
生成部
22
N
第2素数
判定部
14
Yesの場合
N
第1素数
判定部
13
Yesの場合
Noの場合
Noの場合
q, lenq
IDI, lenIDI, c

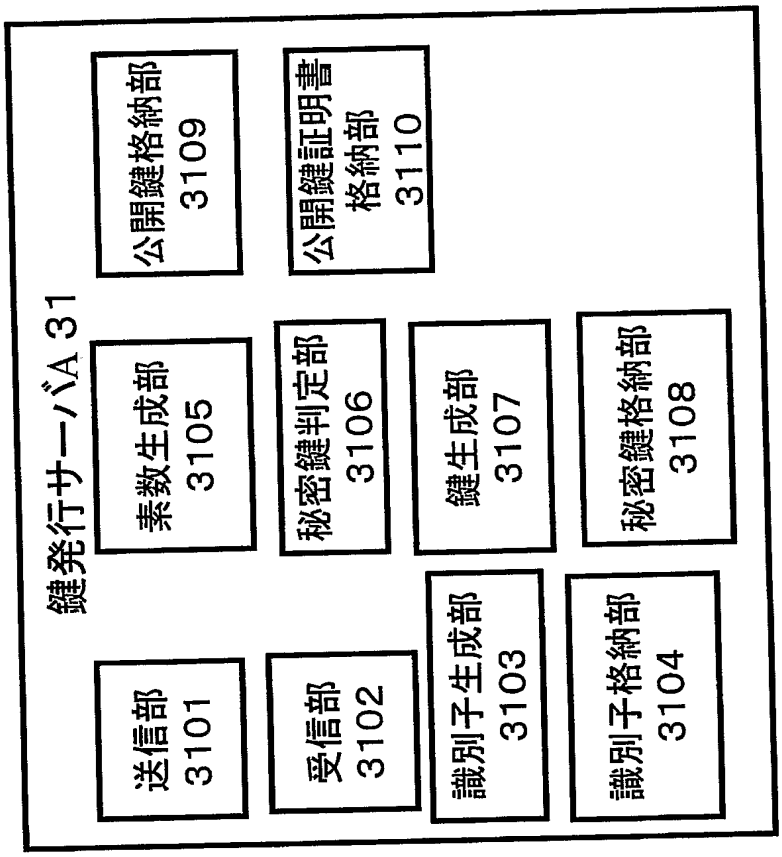
【図４】


Start
S201
乱数生成部11は、T度
(lenq－lenIDI－1)ビットの
乱数R'を生成する。
S202
素数候補生成部22は、
RとNを生成する。
S203
第1素数判定部13は、
2^(N－1) ＝ 1 mod Nの
成立を判定する。
不成立
成立
S204
第2素数判定部14は、
2^(2R) ≠ 1 mod Nの
成立を判定する。
不成立
成立
End

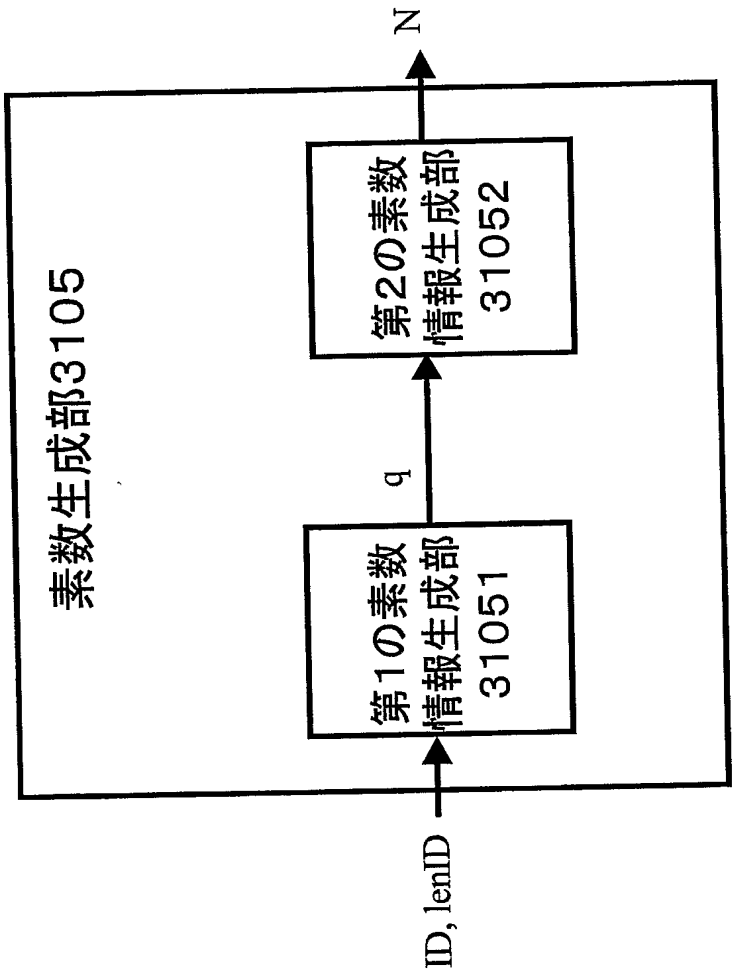
【図５】


鍵発行システム3
証明書発行サーバ
34
鍵発行サーバA 31
鍵発行サーバB 32
鍵発行サーバC 33
端末装置351
端末装置35i
端末装置35n

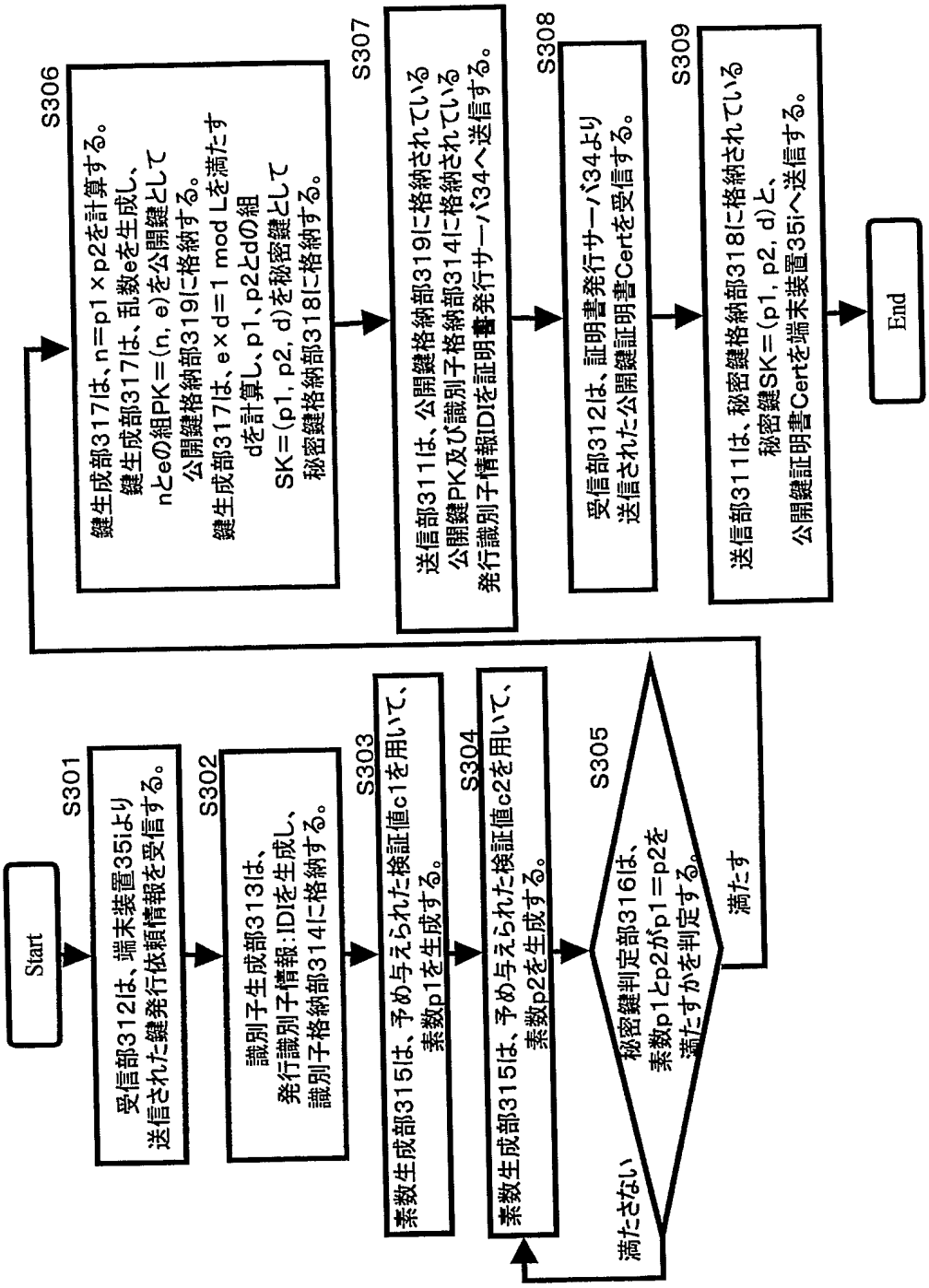
【図６】


鍵発行サーバA 31
送信部 3101
受信部 3102
識別子生成部 3103
識別子格納部 3104
素数生成部 3105
秘密鍵判定部 3106
鍵生成部 3107
秘密鍵格納部 3108
公開鍵格納部 3109
公開鍵証明書格納部 3110

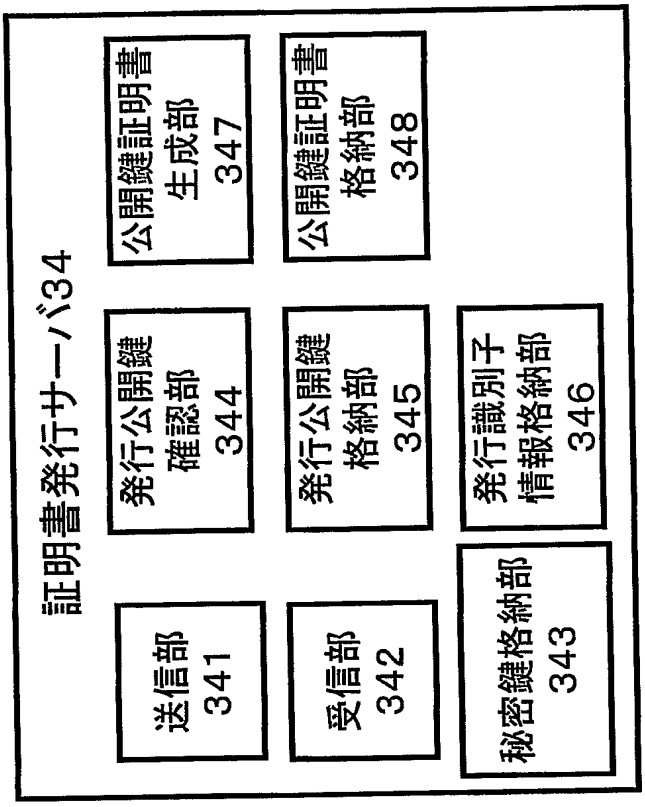
【図７】



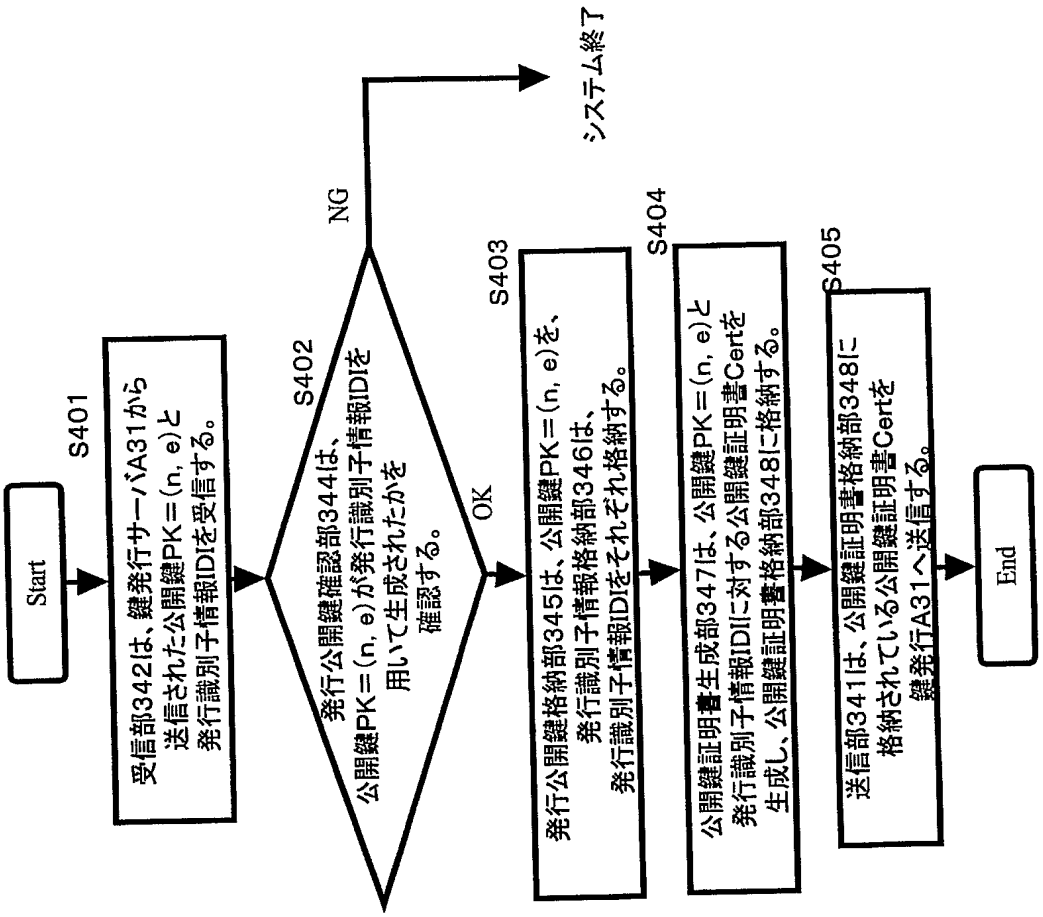
【図８】


Start
S301
受信部312は、端末装置35iより
送信された鍵発行依頼情報を受信する。
S302
識別子生成部313は、
発行識別子情報:IDiを生成し、
識別子格納部314に格納する。
S303
素数生成部315は、予め与えられた検証値c1を用いて、
素数p1を生成する。
S304
素数生成部315は、予め与えられた検証値c2を用いて、
素数p2を生成する。
S305
秘密鍵判定部316は、
素数p1とp2がp1＝p2を
満たすかを判定する。
満たさない
満たす
S306
鍵生成部317は、n＝p1×p2を計算する。
鍵生成部317は、乱数eを生成し、
nとeの組PK＝(n, e)を公開鍵として
公開鍵格納部319に格納する。
鍵生成部317は、e×d＝1 mod Lを満たす
dを計算L、p1、p2とdの組
SK＝(p1, p2, d)を秘密鍵として
秘密鍵格納部318に格納する。
S307
送信部311は、公開鍵格納部319に格納されている
公開鍵PK及び識別子格納部314に格納されている
発行識別子情報IDiを証明書発行サーバ34へ送信する。
S308
受信部312は、証明書発行サーバ34より
送信された公開鍵証明書Certを受信する。
S309
送信部311は、秘密鍵格納部318に格納されている
秘密鍵SK＝(p1, p2, d)と、
公開鍵証明書Certを端末装置35iへ送信する。
End

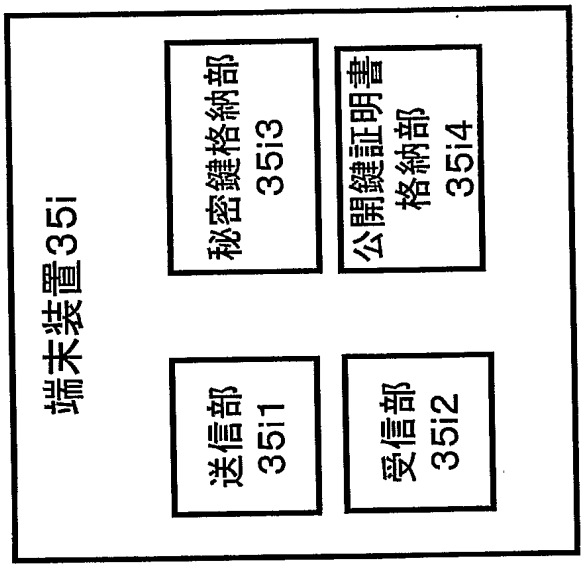
【図９】


証明書発行サーバ34
送信部
341
受信部
342
秘密鍵格納部
343
発行公開鍵
確認部
344
発行公開鍵
格納部
345
発行識別子
情報格納部
346
公開鍵証明書
生成部
347
公開鍵証明書
格納部
348

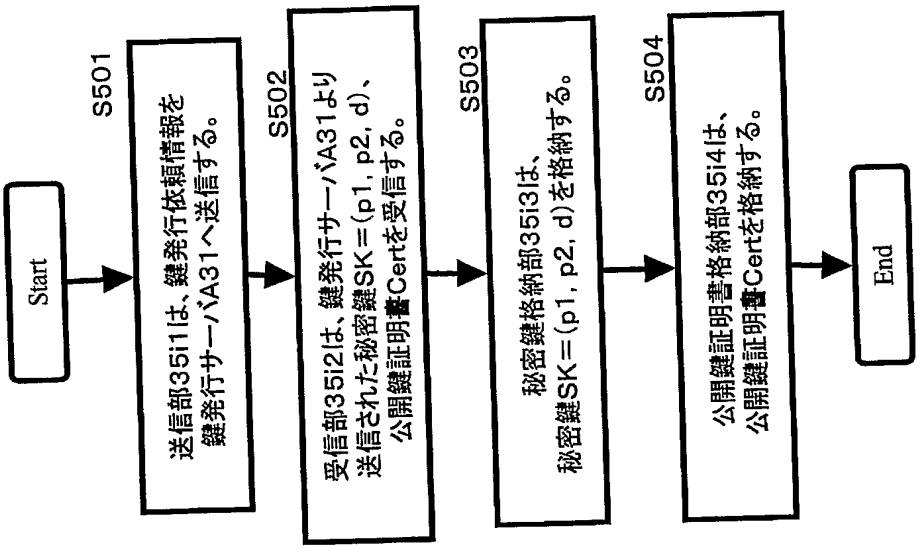
【図１０】


Start
S401
受信部342は、鍵発行サーバA31から送信された公開鍵PK＝(n, e)と発行識別子情報IDIを受信する。
S402
発行公開鍵確認部344は、公開鍵PK＝(n, e)が発行識別子情報IDIを用いて生成されたかを確認する。
NG
システム終了
OK
S403
発行公開鍵格納部345は、公開鍵PK＝(n, e)を、発行識別子情報格納部346は、発行識別子情報IDIをそれぞれ格納する。
S404
公開鍵証明書生成部347は、公開鍵PK＝(n, e)と発行識別子情報IDIに対する公開鍵証明書Certを生成し、公開鍵証明書格納部348に格納する。
S405
送信部341は、公開鍵証明書格納部348に格納されている公開鍵証明書Certを鍵発行A31へ送信する。
End

【図１１】



【図１２】


Start
S501
送信部35i1は、鍵発行依頼情報を鍵発行サーバA31へ送信する。
S502
受信部35i2は、鍵発行サーバA31より送信された秘密鍵SK＝(p1, p2, d)、公開鍵証明書Certを受信する。
S503
秘密鍵格納部35i3は、秘密鍵SK＝(p1, p2, d)を格納する。
S504
公開鍵証明書格納部35i4は、公開鍵証明書Certを格納する。
End

【書類名】要約書
【要約】
【課題】　鍵発行システムで鍵発行サーバを複数もつ場合、鍵発行がシステム全体で正しく行われていることを保証するため、鍵発行システム全体で統一的に同じ鍵発行方法を使用し、管理したいとの要望がある。そこで、鍵発行システムで、鍵発行サーバが正しく鍵発行しているかを判定する方法があればよい。
【解決手段】　鍵発行サーバは、発行識別子を生成する発行識別子生成部と、前記発行識別子情報に基づいて複数の素数を生成する素数生成部と、前記素数を用いて前記秘密鍵及び前記公開鍵を生成する鍵生成部と、を備え、前記端末装置は、前記秘密鍵を格納する秘密鍵格納部と、前記公開鍵を格納する公開鍵格納部と、を備えることにより、素数に発行識別子を埋め込み、発行識別子埋め込みを、公開鍵を用いて確認する。
【選択図】　図５

特願２００３－４３３９０４

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社